PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-145352
(43)Date of publication of application : 29.05.1998

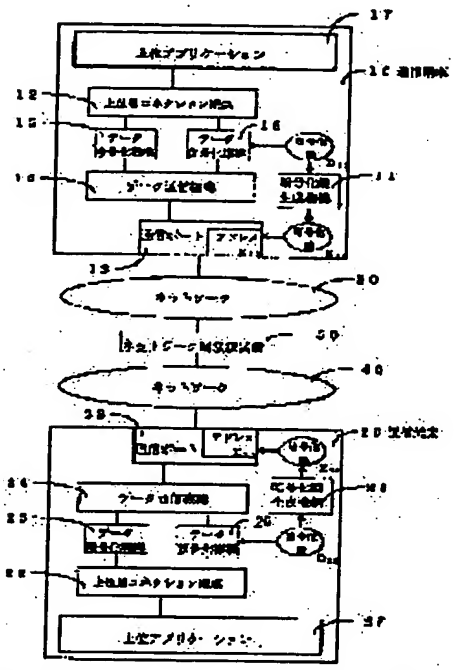
(51)Int.Cl. H04L 9/32
G09C 1/00
H04L 12/28

(21)Application number : 08-300426
(22)Date of filing : 12.11.1996

(71)Applicant : HITACHI LTD
(72)Inventor : YOKOGOSHI KENTARO
OMI MASATO
HAMANAKA NAOTO
TAKAHASHI KOUJI
KAJIWARA KAZUO
TAKIZAWA HIROSHI
MUTO YOSHIYUKI

(54) DATA ENCRYPTION COMMUNICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To enhance the security by conducting encryption in a layer for data communication of a communication terminal equipment in a network of a type sharing a communication medium in common.
SOLUTION: Each of communication terminal equipments 10, 20 prepares definite decoding key data in a system, in which only the terminal equipments 10, 20 themselves are able to recognize. Encryption key data are generated in advance by using the decoding key data, and the public key encryption system and the encryption key data are used for address data of its own communication terminal equipment and kept open to public. In the case of communication between the two communication terminal equipments, the transmitter side communication terminal equipment uses the address data of a communication destination, that is, the encryption key data to encrypt communication text data and provides the address data to the transmission data and sends the resulting data to the network. The receiver side communication terminal equipment analyzes the communication data through the network and receives the data addressed to itself and uses decoding key data, recognizable only to itself for decoding the communication text data.



LEGAL STATUS

[Date of request for examination] 10.03.2000
[Date of sending the examiner's decision of rejection] 09.12.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

* NOTICES *

JPO and NCIPI are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] In case it connects with a network and two or more communication terminals communicate between [on each communication terminal] high order applications The commo data which gave the address data of a communication link place to the correspondence data with which a communication terminal should communicate is sent out in a network. In the data encryption correspondence procedure in the data telecommunication system which receives the commo data addressed to a self-communication terminal by analyzing the address part of the commo data with which the communication terminal of a communication link place is flowing the network Each communication terminal has meaning decryption key data within the system which only a self-communication terminal gets to know. When creating the encryption key data in the end of a local from said decryption key data using a public-key-encryption-ized method, exhibiting this encryption key data as address data of a communication terminal and communicating between [two] communication terminals, The communication terminal which transmits enciphers the correspondence data which should be transmitted using the encryption key data of the partner communication terminal currently exhibited. The data encryption correspondence procedure characterized by giving the encryption key data of a partner communication terminal to this enciphered correspondence data as address data to a partner communication terminal, creating commo data, and sending out this commo data to a network.
[Claim 2] Said communication terminal is a data encryption correspondence procedure according to claim 1 characterized by performing a correspondence data encryption and a decryption by processing of a layer in which not high order application but data communication is performed.
[Claim 3] The encryption key data of each of said communication terminal are a data encryption correspondence procedure according to claim 1 characterized by being stored in the open encryption key directory service equipment connected to the network, and being provided as address data of a communication link place from the name in the end of a communication link head by the demand from each communication terminal.

[Translation done.]

* NOTICES *

JPO and NCIPI are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] A data encryption correspondence procedure is started, and especially, this invention shares the network as communication media, when communicating between [which was connected in the network] communication terminals, it is used in order to communicate by enciphering data, and relates to a suitable data encryption correspondence procedure.
[0002]
[Description of the Prior Art] In case it communicates between communication terminals in recent years, between communication terminals is not connected to 1 to 1 by the circuit of dedication, but the network as communication media is shared, and the data telecommunication system with which the communication terminal connected to the network communicates mutually through a network is put in practical use.
[0003] A network as communication media which was mentioned above is shared, and the technique indicated by IEEE802.3 is known as a conventional technique about the communication link between terminals connected to the network.
[0004] This conventional technique cancels the commo data reception and whose address part are not addressing to self-equipment about the commo data addressed to a self-communication terminal, when the commo data with which the layer which performs data communication gave the address data of a communication link place to the correspondence data received from the layer of a high order is created, it is sent out to a network and the communication terminal connected to the network analyzes the address part of the commo data which flows a network.
[0005] And there are especially no criteria about whether the above-mentioned conventional technique is performed by the application whose communication link data encryption is not the layer that performs data communication but the layer of a high order, and it enciphers also in the layer of a high order, and how to include an encryption device in each application uniquely is taken to keep secrecy between each application.
[0006]
[Problem(s) to be Solved by the Invention] When the data encryption correspondence procedure by the conventional technique mentioned above communicates, the correspondence data encryption is not performed in the layer which performs data communication and the correspondence data encryption is not performed by the application of a high order, address data will be given to the correspondence data which are not enciphered as it is, and they will be sent out on a network. For this reason, that the communication terminal on a network misrepresents the address, or by using a protocol analyzer etc., said conventional technique is intercepted by other communication terminals, and has the trouble that there is a possibility that an inaccurate partner may receive correspondence data.
[0007] Although it must encipher with the application of a high order in order to solve such a trouble, the trouble that the encryption device must be uniquely incorporated for every application in this case for encryption is produced.
[0008] The object of this invention is to offer the data encryption correspondence procedure which enabled the consolidation of the security in a communication link, without needing modification of the specification of the layer of the application of a high order by solving the trouble of said conventional technique and enciphering correspondence data in the layer which performs data communication.
[0009]
[Means for Solving the Problem] According to this invention, said object enciphers correspondence using a public-key-encryption-ized method in the layer which performs data communication, and is attained by using encryption key data as the address of a communication link place as it is.
[0010] In addition, the paper by W.Diffie and M.Hellman which are indicated by "OPENDESIGN No.14 pp 23-26" is known, concerning the principle of a public-key-encryption system.
[0011] According to said paper, a public-key-encryption system is made into two kinds of commutative conversion methods in message space {M}, and the following formula can express it.
EK: {M} -> {M}
DK: {M} -> {M}
And these formulas fulfill the following properties.
[0012] (1) EK and DK are inverse transformation about all the keys K.

(2) The conversion by EK and DK is easily calculable about all the keys K and M.
(3) It is dramatically difficult to calculate DK from EK about the key K of all ********.
(4) It is easy to ask for the pair of EK and DK from Key K about all the keys K.
[0013] By finding EK and DK with a property which was mentioned above, it becomes possible to realize a public-key-encryption system by making into encryption algorithm EK calculated from a certain key K, and making DK into a decryption algorithm. Moreover, even if it exhibits encryption algorithm EK with the above-mentioned property (3), it is dramatically difficult to ask for the decryption algorithm DK, and it can maintain security.
[0014] A public-key-encryption-ized method which was mentioned above is used for this invention. And as for the object of said this invention, two or more communication terminals are connected to a network. In case it communicates between [on each communication terminal] high order applications, the commo data which gave the address data of a communication link place to the correspondence data with which a communication terminal should communicate is sent out in a network. In the data encryption correspondence procedure in the data telecommunication system which receives the commo data addressed to a self-communication terminal by analyzing the address part of the commo data with which the communication terminal of a communication link place is flowing the network It has meaning [within the system which only a self-communication terminal gets to know] communication terminal [each] decryption key data. When creating the encryption key data in the end of a local from said decryption key data using a public-key-encryption-ized method, exhibiting this encryption key data as address data of a communication terminal and communicating between [two] communication terminals, The correspondence data which the communication terminal which transmits should transmit using the encryption key data of the partner communication terminal currently exhibited are enciphered. The encryption key data of a partner communication terminal are given to this enciphered correspondence data as address data to a partner communication terminal, commo data is created, and it is attained by sending out this commo data to a network.
[0015] moreover, the thing for which the object of said this invention performs a correspondence data encryption and a decryption by processing of a layer in which said communication terminal performs not high order application but data communication — moreover, it stores in the open encryption key directory service equipment by which the encryption key data of each of said communication terminal were connected to the network, and is attained by providing as address data of a communication link place from the name in the end of a communication link head by the demand from each communication terminal.
[0016] Other communication terminals connected to the same network as the communication terminal of a receiving side by having the above-mentioned configuration this invention Also when the commo data addressed to the communication terminal of a receiving side which misrepresents the address data of the communication terminal of the receiving side currently exhibited, and is flowing the network is monitored, other communication terminals Since it does not have in normal decryption key data for the communication terminals which only the communication terminal which receives data can know, cipher data cannot be decoded to correspondence data.
[0017] Thereby, it becomes possible to strengthen security in the layer which performs data communication, without this invention changing the specification of the application layer of a high order.
[0018]
[Embodiment of the Invention] Hereafter, a drawing explains 1 operation gestalt of the data communication code approach by this invention to a detail.
[0019] The block diagram showing the configuration of 1 operation gestalt of the data encryption communication system with which drawing 1 applied this invention, and drawing 2 are the flow charts explaining actuation of the data communication processing in the system shown in drawing 1 . drawing 1 — setting — 10 and 20 — a communication terminal, and 11 and 21 — an encryption key generation device, and 12 and 22 — an upper layer connection endpoint, and 13 and 23 — as for high order application, and 30 and 40, for a data encryption device, and 16 and 26, a data decryption device, and 17 and 27 are [a data communication device, and 15 and 25 / a communication link port, and 14 and 24 / a network and 50] internetwork contacts.
[0020] The system by 1 operation gestalt of this invention shown in drawing 1 is constituted by the communication terminal 10 connected to the network 30, the communication terminal 20 connected to the network 40, and a network 30 and the internetwork contact 50 which connects between 40. In addition, although two communication terminals are shown in drawing 1 , it cannot be overemphasized that many communication terminals are actually connected further to networks 30 and 40. Moreover, although two networks connected to mutual [which has held the communication terminal] also about the network are shown in drawing 1 , you may be only the large-scale network where the network beyond it was actually connected to multistage mutually, or one network where the communication terminal was connected mutually.
[0021] Communication terminals 10 and 20 are equipped with the encryption key generation devices 11 and 21, the upper layer connection endpoints 12 and 22, the communication link ports 13 and 23, the data communication devices 14 and 24, the data encryption devices 15 and 25, the data decryption devices 16 and 26, and the high order applications 17 and 27, respectively, and are constituted. And although [the communication terminal of 1 operation gestalt of this invention shown in drawing 1] high order application is equipped only with one, ** is also good even if it carries much applications in a communication terminal. Moreover, the communication terminals 10 and 20 in 1 operation gestalt of this invention have decryption key data as D10 and D20, respectively, presuppose that these decryption key data D10 and D20 are mutually made secrecy, and are performing them in the layer which performs data communication between application and a network for the correspondence data encryption which used these key data, and a decryption.

[0022] The encryption key generation devices 11 and 21 have the function which generates the encryption key data corresponding to the decryption key data D10 and D20, and generate the encryption key data E10 and E20 of each communication terminal 10 and 20 from the decryption key data D10 and D20 of each communication terminal. At this time, the encryption function f (T, E) and the decryption function g (T, D) shall have the relation of g(T, DK) = f-1 (T, EK), i.e., the relation of inverse transformation, to all the keys K.
[0023] The upper layer connection endpoints 12 and 22 transmit the correspondence data with which the high order applications 17 and 27 perform the communication link with the application of a communication link place, and its communication link place between the applications 17 and 27 of the upper layer, and the data communication devices 14 and 24, and have division or the function which assembles a bit string to correspondence data in the bit string of the suitable die length for which the data communication devices 14 and 24 use correspondence data as a transmitting unit.
[0024] The communication link ports 13 and 23 are the end connections for connecting networks 30 and 40 and communication terminals 10 and 20, and have the address data of a proper within a system. In the communication link ports 13 and 23, 1 operation gestalt of this invention has E10 and E20 as address data, respectively, using the encryption key data E10 and E20 of a communication terminal proper as these address data.
[0025] It has the function to supervise the commo data which the data communication devices 14 and 24 give the address data of a communication link place to the enciphered cipher data, and sends them out to a network, or is flowing the network, to receive the commo data addressed to a self-communication terminal, to delete address data, and to extract cipher data.
[0026] The data encryption devices 15 and 25 have the function which creates cipher data using the encryption key data for the communications-partner points currently exhibited in correspondence data and the address data of a communication link place, and the data decryption devices 16 and 26 have the function which decrypts correspondence data using cipher data and its own decryption key data.
[0027] It has the function which all the communication terminals by which the received commo data is connected to the self-network transmit networks 30 and 40 to ability ready for receiving, and the internetwork contact 50 connects a network mutually, analyzes the address part of commo data, and carries out routing of the commo data to a suitable network.
[0028] Next, it explains with reference to the flow which shows processing actuation of the data communication by the data encryption communication system which applied this invention which has the configuration mentioned above to drawing 2 . In addition, the flow shown in drawing 2 is an example of operation in case a communication terminal 20 serves as a communication link place and a communication link is performed communication terminal's 10 communication link origin.
[0029] (1) Suppose that the communicative demand occurred in the high order application 17 on a communication terminal 10 between the high order applications 27 on a communication terminal 20, and the communication link of correspondence data was needed for it a communication terminal 10 and between 20 now. It is the correspondence data T (10-20) which transmit the high order application 17 to a communication terminal 20 from a communication terminal 10 to the upper layer connection endpoint 12 at this time. And the address data E20 of the communication link port 23 of the communication terminal 20 which is a communication link place are transmitted. By this the upper layer connection endpoint 12 in a communication terminal 10 received correspondence data T (10-20) n correspondence data T (10-20) (i) in which the data communication device 14 has the bit string of suitable die length used as a transmitting unit -- [-- however It divides into i= 1 - n], and these correspondence data T (10-20) (i) and the encryption key data E20 for communication terminal 20 as address data of the communication link port 23 of the communication terminal 20 which is a communication link place are sent to the data encryption device 15 (step 101).
[0030] (2) The data encryption device 15 each of correspondence data T (10-20) (i) received from the upper layer connection endpoint 12 It enciphers using the algorithm f (T, E) beforehand defined using the encryption key data E20 for communication terminal 20 as address data of the communication link port 23 of the communication terminal 20 which is a communication link place. Cipher data C(20 10- 20) (i) =f (T (10-20) (i), E20) is created. The data encryption device 15 sends the cipher data C (20 10- 20) (i) which enciphered to the data communication device 14 (step 102).
[0031] (3) The data communication device 14 gives the address data E20 of the communication link port of the communication terminal 20 which is a communication link place to the received cipher data as address part, and creates commo data F20(i) =E20+C (20 10- 20) (i) (step 103).
[0032] (4) The data communication device 14 sends out the created commo data F20 (i) to a network 30 through the communication link port 13 (step 104).
[0033] (5) All the communication terminals by which the received commo data F20 (i) is connected to the network 30 transmit to ability ready for receiving, the internetwork contact 50 connected to the network 30 analyzes the address part of the received commo data F20 (i), and a network 30 sends out commo data F20 (i) to the network 40 where the communication device 20 which is a communication link place is connected (step 105).
[0034] (6) The data communication device 24 in a communication terminal 20 is supervising all commo data F that flows a network 40 through the communication link port 23 connected to the network 40, analyzes address part E of all commo data F, and when address part E is not the address data E20 of its communication link port 23, it discards the data (steps 106 and 107).
[0035] (7) When address part E is the address data E20 of its communication link port 23, the data communication

device 24 interprets the commo data F as it being commo data F<SUB>20(i) addressed to a self-communication terminal, and receives the commo data (step 107).
[0036] (8) The data communication device 24 deletes E20 which is address part from the received commo data F20 (i), takes out the cipher data C (20 10- 20) (i), and sends them to the data decryption device 26 (step 109).
[0037] (9) The data decryption device 26 decrypts the cipher data C (20 10- 20) (i) using the algorithm g (T, D) beforehand defined using the decoding key data D20 for cipher data [which were received] C (20 10- 20) (i) and end of local, i.e., communication terminal, 20. As decode sentence data T (bit string T10-20(i to which, as for i), the data communication device divided correspondence data into the suitable die length used as a transmitting unit) T (i) =g (C (20 10- 20) (i), D20)
= g (f (T10-20(i), E20), D20)
= f-1 (f (T10-20(i), E20), E20)
= T10-20 (i)
** — it asks like (step 110).
[0038] (10) bit string T from which the data decryption device 26 was extracted — bit string T which sent 10-20 (i) to the upper layer connection endpoint 22, and the upper layer connection endpoint 22 received — assemble 10-20 (i), create correspondence data T10-20, and transmit to the high order application 27 (step 111).
[0039] Although the data encryption communication system which applied this invention operated as mentioned above, now, temporarily, other communication terminals connected to the same network as a communication terminal 20 should misrepresent the address data of the communication link port in the end of a local as their being the address data E20 of the communication link port 23 of the communication terminal 20 currently exhibited, and it should monitor the commo data F20 addressed to communication terminal 20 (i). in this case — since other communication terminals which misrepresented address data do not have the decryption key data D20 for communication terminal 20 made into secrecy -- the cipher data C (20 10- 20) (i) — the correspondence data T — it cannot decode to 10-20 (i), but security can be kept certain — there is nothing.
[0040] Although it explained that each communication terminal exhibited the encryption key of a self-communication terminal as address data, 1 operation gestalt of this invention mentioned above may constitute this invention so that it may carry out from the identifier of a communication link place into a network by having open cryptographic key directory service equipment which serves the encryption key data which are the address data of a communication link place as the same layer as the layer which performs data communication [in / for disclosure of the encryption key of this communication terminal / drawing 1]. In this case, what is necessary will be to need a transmitter style with a open cryptographic key directory service in a communication terminal, and just to tell correspondence data and the identifier of a communication link place as data which tell an upper layer connection endpoint from high order application.
[0041]
[Effect of the Invention] As explained above, a communication terminal can encipher correspondence data easily in the layer which performs data communication only by getting to know the address in the end of a communication link head, without changing the specification of the application layer of the high order in a communication terminal in a data telecommunication system according to this invention, and when commo data is received by the inaccurate partner, the confidentiality of correspondence data can be held.

[Translation done.]